UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/828,559	04/06/2001	Osamu Shibata	29288.0300	6490

20322 7590 02/27/2007
SNELL & WILMER L.L.P. (Main)
400 EAST VAN BUREN
ONE ARIZONA CENTER
PHOENIX, AZ 85004-2202

EXAMINER	
HOMAYOUNMEHR, FARID	
ART UNIT	**PAPER NUMBER**
2132	

SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE
3 MONTHS	02/27/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

Office Action Summary	Application No.	Applicant(s)	
	09/828,559	SHIBATA ET AL.	
	Examiner	Art Unit	
	Farid Homayounmehr	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *07 December 2006*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-47* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-47* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This action is responsive to amendments filed 12/7/06. All previous office actions are incorporated by reference.

2. Claims 1-47 are pending in the case.

Response to Arguments

3. Applicant argues: "In particular, the Examiner fails to fully address the arguments presented by the Applicants submitted in reply to the previous Office Action. However, Examiner's office actions have clearly identified examples of elements of Ishibashi that corresponds to each element of claimed limitations, and explain in detail the reasons applicant's arguments are not persuasive.

Applicant also argues that Examiner no longer alleges item 14 of Ishibashi to be analogous to "the first contents key generation section" and simply refers to item 100 of Ishibashi. However, item 14 is a content key generation section, which produces Kcd. In addition to item 40, item 100 includes item 131, which is also a content key generation section, producing Kcd, by decrypting the encrypted Kcd. As mentioned before, Kcd is produced based on a copy control code (decryption limitation), as indicated in, for example, previously cited column 6 line 1 to 20.

Applicant also argues: "As also previously argued, claim 1 recites "*the encryption device includes ... **a first** contents key generation section for generating the contents key based on a second decryption limitation ... and ... a decryption device includes **a second** contents key generation section for generating the contents key from the second decryption limitation*" (emphasis added). However, the Examiner fails to address such arguments and simply alleges that the Applicants present no supportive argument to traverse the Examiner's rejections (see page 2, 6th paragraph of Advisory Action). Contrary to the Examiner's allegation, Applicants clearly provided supportive arguments by stating that Ishibashi fails to teach the aforementioned features of claim 1." However, Examiner has shown how Ishibashi teaches the limitations of the mentioned claim in the previous office action by citing the relevant portions of Ishibashi. Applicant has not provided any supporting argument against the rejection, except for stating that Ishibashi fails to teach the aforementioned features of claim 1. Stating that Ishibashi fails to teach the limitations is not a valid argument against the existing rejection.

Applicant further argues that the claim requires two content key generation sections, one in the encryption device and the other in the decryption device. Applicant simply states that the elements are not disclosed by Ishibashi. However, previous office actions clearly disclose how the limitations are taught by Ishibashi. The teachings of Ishibashi relative to the two content key generation sections is also discussed in the next section of this office action.

With regards to claim 14, applicant argues that items 100 and 200 do not have a contents encryption unit. However, claim rejection cites item 16 of device 10 as the item that encrypts the contents data.

With regards to claim 26, applicant once again argues that the contents key of Ishibashi is not generated from the second decryption limitation. However, as stated before, Ishibashi's key is updated based the copy code, which represents the second decryption limitation.

Applicant further argues that the decryption section for decrypting encrypted contents using the contents key generated by the contents key generation section of claim 26 must be part of **a** decryption device and it is impermissible to pick and choose the elements. However, item 100, for example, includes all the mentioned limitations on the same device as discussed in the next section.

Applicant has amended the claims to include new limitation. The new limitations are discussed in the new rejection, outlined in the next section.

Claim Objections

4. Claims 1, 14, 26, and 37 are objected to because of the following informalities: Mentioned claims include the phrase "the second encrypted decryption limitation". There is no antecedent basis for "the second encrypted decryption limitation". For the purpose of this examination, "the second encrypted decryption limitation" is interpreted as encrypted decryption limitation based on applicant's comments (see applicant's remarks, dated 12/7/06, page 17), and rejected accordingly. Corrective action is required.

Claim Rejections - 35 USC § 103

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

6. Claims 1-47 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ishibashi (U.S. Patent No. 6,728,379 B1, filed July 28, 1999).

6.1. As per claim 1, Ishibashi is directed to a copyright protection system (column 1 line 22 to 25) comprising: an encryption device (item 10 and associated text. Items 100 and 200 also perform encryption) and a decryption device (Information Processors 100 and 200 both perform decryption), wherein cryptographic communication is performed between the encryption device and the decryption device (Figures 2 and 3 and the associated texts) using a contents key (Kce and Kcd as shown in Figures and

associated text. Also note that public key encryption, (which uses separate keys for encryption and decryption) can be replaced by private (symmetric) key encryption, which uses one key for both encryption and decryption, as indicated in col. 4 line 34 to 42), wherein the encryption device includes a contents storage section for storing contents (item 11 of Fig. 8 and associated text), a first contents key generation section for generating the contents key (item 14 of Fig. 8 and associated text, also see column 4 line 24 to 33) based on a second decryption limitation obtained by updating a first decryption limitation (column 6 line 1 to 20 discloses SCMS as an example system of a copy control scheme that uses control codes in set in the content and the associated encryption keys for copy control. Also note that the process of updating the content key based on the copy control code and client usage and purchase of content is clearly disclosed in col. 9 line 52 to col. 13 line 60. The process is explained within item 100, but it would have been obvious to a person skilled in art to perform the same in item 10 (content provider), where the content key is generated. The motivation is to allow the content provider to control the copying of the content), and a first encryption section for encrypting the contents using the contents key (item 13 Fig. 8) and outputting the encrypted contents (item 15 Fig. 8), and wherein the decryption device includes a second contents key generation section for generating the contents key from the second decryption limitation (item 131 of Fig. 8 generates Kcd, which is used to decrypt the content. As the content was encrypted based on a copy control scheme, namely SCMS, the copy control code was updated and embedded in the content or the key (see column 10 line 53 to 66 and also column 13 line 47 to 60), accordingly) and a first

decryption section for decrypting the encrypted contents using the contents key generated by the second contents key generation section (item 136 of Fig. 8 and associated text), wherein the encryption device further includes a third encryption section for encrypting the first decryption limitation using a time-varying key and outputting the second encrypted decryption limitation to the decryption device (the copy control data (encryption limitation) is buried in content data (see, for example, col. 1 line 1-5), and all the communication between devices is encrypted by a session key (see, for example, col. 9 line 3-10, or col. 10 line 60 to col. 13 line 47), which is a time-varying key), and the decryption device further includes a third decryption section for decrypting the second encrypted decryption limitation transferred from the third encryption section using the time-varying key and outputting the first decryption limitation (all communication is encrypted by a session key as explained above. Also see Fig. 6 and associated text).

6.2. As per claim 2, Ishibashi is directed to a copyright protection system according to claim 1, wherein the decryption device further includes a decryption limitation updating section for updating the first decryption limitation to the second decryption limitation in accordance with a decryption limitation updating rule (column 12 line 4 to 15), and a second encryption section for encrypting the second decryption limitation using a time-varying key (column 12 line 33 to 43), and outputting the first encrypted decryption limitation, wherein the encryption device further includes a second decryption section for decrypting the first encrypted decryption limitation transferred from the second

encryption section using the time-varying key to generate the second decryption limitation, wherein the first contents key generation section generates the contents key based on the second decryption limitation generated by the second decryption section (column 13 line 15 to 26. Note that the Content provider and the information system 100 also perform the SCMS method for inclusion of the copy control code to limit number of allowable copies at item 100. Therefore, content encryption and key generation at the content provider also involves updating encryption keys based on the control code and in accordance with the copy rights updated at the information center.).

6.3. As per claim 3, Ishibashi is directed to a copyright protection system according to claim 2, wherein the encryption device further includes a first common key storage section for storing a common key (column 9 line 4 to 10 discloses a mutual authentication between all elements in Fig. 8. Furthermore, the said mutual authentication is described in column 7 lines 33 to 65. Therefore, the content provider executes a mutual authentication method, namely ISO/IEC 9798-3, which will require establishment of a common key, and a location for storage), a decryption limitation storage section for storing the first decryption limitation (as described in response to claim 2, the content provider performs SCMS in association with the item 100 to establish a copy code, and therefore stores a copy code, which is updated in sync with item 100), a first random number generation section for generating a first random number, a first mutual authentication section for performing mutual authentication in association with the decryption device using the first random number, and a second

random number transferred from the decryption device, a first time-varying key generation section for generating the time-varying key using the first random number and the second random number in response to the authentication by the first mutual authentication section (random number generation and exchange between two parties performing mutual authentication, and establishment of a session key, are part of a mutual authentication method, namely ISO/IEC 9798-3 performed between the content provider and item 100, as described in Fig. 6 and the associated text, and also column 5 lines 5 to 21), and wherein the decryption device further includes a second common key storage section for storing the common key, a second random number generation section for generating the second random number, a second mutual authentication section for performing mutual authentication in association with the encryption device using the second random number and the first random number, a second time-varying key generation section for generating the time-varying key using the second random number and the first random number in response to the authentication by the second mutual authentication section (again, item 100 performs SCMS for receiving the copy codes using a session key obtained thorough a mutual authentication).

6.4. As per claims 4 and 5 Ishibashi is directed to a copyright protection system according to claim 1, wherein the decryption device further includes a first decryption limitation updating section for updating the first decryption limitation to the second decryption limitation in accordance with a decryption limitation updating rule (column 6 lines 1 to 20), and a second contents key generation section for generating the contents

key based on the second decryption limitation updated by the first decryption limitation updating section (column 10 line 42 to column 11 line 9), wherein the encryption device further includes a second decryption limitation updating section for updating the first decryption limitation to the second decryption limitation in accordance with the decryption limitation updating rule in response to the updating of the first decryption limitation by the first decryption limitation updating section, the first contents key generation section generates the contents key based on the second decryption limitation updated by the first decryption limitation updating section (the content provider and Information Processing Unit 200 both perform SCMS and implement copy code updating and secure exchange of the copy code).

6.5. As per claim 6, Ishibashi is directed to a copyright protection system according to claim 5, wherein the second decryption limitation updating section updates the first decryption limitation to the second decryption limitation in advance (column 10 lines 9 to 26 discloses the case when the content decryption and distribution decryption keys are supplied by the Key Distribution Center, item 30, and therefore are supplied in advanced), the first contents key generation section generates the contents key from the second decryption limitation, and the second decryption limitation updating section stores the second decryption limitation in the decryption limitation storage section in response to the start of processing by the first encryption section (see responses to claim 3 and 4).

6.7. As per claim 7, Ishibashi is directed to a copyright protection system according to claim 3, wherein the first and second time-varying key generation sections generate the time-varying key based on the first and second random numbers and the common key (time varying keys, and their generation is disclosed in method ISO/IEC 9798-3 for mutual authentication. See column 7 line 37).

6.8. As per claim 8, Ishibashi is directed to a copyright protection system according to claim 3, wherein the first and second contents key generation sections generate the contents key based on the second decryption limitation and the time-varying key (see response to claims 45 and 5).

6.9. As per claim 9, Ishibashi is directed to a copyright protection system according to claim 3, wherein the encryption device and the decryption device further include respective first and second data sequence key generation sections for generating a data sequence key based on a data sequence input to or output from the encryption device and the decryption device, and wherein the first and second time-varying key generation sections generate the time-varying key based on the first and second random numbers and the respective data sequence key(as described in column 13 lines 57 to 60 and column 14 lines 22 to 24, alternative and more comprehensive methods to secure the exchange of keys between the parties may be deployed. Sequence key generation is a well-known method to synchronize receiver and transmitter engaged in secure data transmission and improve the strength of encryption, as described in text

books such as Bruce Schneier's Applied Cryptography, ISBN 0-471-11709-9, (see section 9.5). Ishibashi's disclosure of mutual authentication implies use of well-known methods to perform mutual authentication, such as sequence key generation).

6.10. As per claim 10, 11, 12 Ishibashi is directed to a copyright protection system according to claim 3, wherein the encryption device and the decryption device further include respective first and second data sequence key generation sections for generating a data sequence key based on a data sequence input to or output from the encryption device and the decryption device, and wherein the first and second time-varying key generation sections generate the time-varying key based on the first and second random numbers, the common key, and the respective data sequence key (see response to claims 9, 3 and 4).

6.10. As per claim 13, Ishibashi is directed to a copyright protection system according to claim 3, wherein the first and second mutual authentication sections mutually authenticate the decryption device and the encryption device, respectively, by communication in accordance with a challenge-response type authentication protocol (as described in column 13 lines 57 to 60 and column 14 lines 22 to 24, alternative and more comprehensive methods to secure the exchange of keys between the parties may be deployed. Challenge-response is a well-known method to establish mutual authentication between parties, as described in text books such as Bruce Schneier's Applied Cryptography, ISBN 0-471-11709-9, (see section 3.2, page 54). Ishibashi's

disclosure of mutual authentication implies use of well-known methods to perform mutual authentication, such as sequence key generation).

6.14. As per claim 14, Ishibashi is directed to an encryption device for performing cryptographic communication in association with a decryption device using a contents key, comprising: a contents storage section for storing contents (fig. 8 item 11); a second encryption section for encrypting the first decryption limitation using a time-varying key and outputting the second encrypted decryption limitation to the decryption device (see response to claim 1); a contents key generation section (item 14) for generating the contents key based on a second decryption limitation obtained by updating a first decryption limitation (column 6 lines 1 to 20, column 10 lines 53 to 66, and column 12 lines 25 to 44 disclose Ishibashi's use of SCMS, which controls the number of copies made from copyright protected material by updating limitations of copy codes in the content data and keys); and a first encryption section for encrypting the contents using the contents key and outputting the encrypted contents (item 16).

6.15. As per claims 15 to 25 Ishibashi is directed to an encryption device according to claim 14 (item 100 in Fig. 8 discloses both encryption and decryption devices, as it receives the encrypted content data from item 10, decrypts it to extract the content, and re-encrypts it in accordance with the copy control code (copy limitation) and sends it to item 200 (another Information Center), which perform decryption. As described in responses to claims 1 to 13, this process is secured by mutual authentication between

items 10, 100, 200 and other elements in Fig. 8. Mutual authentication involves the use of encryption techniques such as time-varying keys, random number generation and use for key generation, challenge–response protocol, data segmentation, etc. Ishibashi also discloses SCMS method for copy control. In the following, the encryption device is disclosed by item 100, and decryption device is disclosed by item 200. Item 100 does disclose all the elements of claim 14, as it includes and encryption section, and performs SCMS to update the copy code sent to item 200), further including a decryption section for decrypting the first encrypted decryption limitation transferred from the decryption device (item 131) using the time-varying key to generate the second decryption limitation, and the contents key generation section generates the contents key based on the second decryption limitation generated by the decryption device (item 133 and the associated text, also see responses to claims 1 to 14).

6.16. As per claim 26, Ishibashi is directed to a decryption device (Fig. 8 item 100 or 200) for performing cryptographic communication in association with an encryption device (item 100 or 10) using a contents key, comprising: a second decryption section for decrypting a second encrypted decryption limitation transferred from the encryption device using the time-varying key and outputting a first decryption limitation (see response to claim 1); a decryption limitation updating section for updating a first decryption limitation to a second decryption limitation in accordance with a decryption limitation updating rule (the copy control mechanism as discussed in claim 1 in item 200, which performs SMCS protocol which includes updating a copy code, as described

in column 6 line 1 to 20); a contents key generation section for generating the contents key from a second decryption limitation (item 231 generates the key to decrypt the content decryption key, which in accordance with SMCS includes a copy code (decryption limitation); and a first decryption section for decrypting encrypted contents using the contents key generated by the contents key generation section (item 236 and the associated text).

6.17. As per claims 27 to 36 Ishibashi is directed to a decryption device according to claim 26, further including an encryption section for encrypting the second decryption limitation using a time-varying key, and outputting the first encrypted decryption limitation (item 200 performs SMCS protocol which includes updating a copy code, as described in column 6 line 1 to 20).

6.18. As per claims 37 to 47, Ishibashi is directed to a recording medium storing a program for use in causing a computer to perform cryptographic communication with an encryption device (Fig. 8 item 100), a second decryption section for decrypting a second encrypted decryption limitation transferred from the encryption device using the time-varying key and outputting a first decryption limitation (see response to claim 1); a decryption limitation updating section for updating a first decryption limitation to a second decryption limitation in accordance with a decryption limitation updating rule (the copy control mechanism as discussed in claim 1 in item 200, which performs SMCS protocol which includes updating a copy code, as described in column 6 line 1 to 20);

using a contents key, wherein: the program causes the computer to function as: a contents key generation section for generating the contents key from a second decryption limitation (item 133, as described in response to claim 15); and a first decryption section for decrypting encrypted contents using the contents key generated by the contents key generation section (item 131 as explained in response to claim 15, and response to claims 1 to 16).

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Farid Homayounmehr whose telephone number is 571 272 3739. The examiner can normally be reached on 9 hrs Mon-Fri, off Monday biweekly.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on (571) 272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Farid Homayounmehr

Examiner

Art Unit: 2132